



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT

Avoidable Software Procurements

By: **Raymond K. Koshi**
 Kenneth C. Robinson
 September 2012

Advisors: **Brad R. Naegle**
 Charles K. Pickar
 Christina M. Kelton

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2012	3. REPORT TYPE AND DATES COVERED Joint Applied Project	
4. TITLE AND SUBTITLE Avoidable Software Procurements			5. FUNDING NUMBERS	
6. AUTHOR(S) Raymond K. Koshi, Kenneth C. Robinson				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The United States Department of Defense (DoD) spends billions of dollars a year in acquiring software of which a great deal never gets used. Although a large portion of that software is sole source, a considerable savings may be had in development of a check-in/check-out (CICO) system for software. Such a system could be likened to a library or a video-rental model. The purpose of this Joint Applied Project (JAP) was to explore and offer a broad examination of the cost of commercial software usage in the United States Department of Defense. Through an analysis of cost usage data, we propose that potential significant cost savings in commercial software procurement can be accomplished through a check-in/check-out (CICO) system.				
14. SUBJECT TERMS Asset Discovery Tool, ADT, Army Data Center Consolidation Plan, ADCCP, check-in, check-out, cloud computing, commercial software procurement, COTS software procurement, data center consolidation, enterprise license agreement, ELA, software license, software usage, ELA, Software as a Service, SaaS, Software Asset Management, SAM.			15. NUMBER OF PAGES 53	
			16. PRICE CODE N/A	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

AVOIDABLE SOFTWARE PROCUREMENTS

Raymond K. Koshi, Civilian, United States Army, JCISA-P, 1st Signal Brigade,
U.S. Army Garrison Yongsan, Seoul, South Korea

Kenneth C. Robinson, Civilian, United States Army, CECOM-LCMC, Software
Engineering Center, Aberdeen Proving Ground, Maryland

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
September 2012**

Authors:

Raymond K. Koshi

Kenneth C. Robinson

Approved by:

Brad R. Naegle, Lead Advisor

Charles K. Pickar, Support Advisor

Christina M. Kelton, Support Advisor

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

Avoidable Software Procurements – An assessment of a check-in/check-out system for Commercial-Off-The-Shelf (COTS) software used in Department-of-Defense (DoD) office automation

ABSTRACT

The United States Department of Defense (DoD) spends billions of dollars a year in acquiring software of which a great deal never gets used. Although a large portion of that software is sole source, a considerable savings may be had in development of a check-in/check-out (CICO) system for software. Such a system could be likened to a library or a video-rental model.

The purpose of this Joint Applied Project (JAP) was to explore and offer a broad examination of the cost of commercial software usage in the United States Department of Defense. Through an analysis of cost usage data, we propose that potential significant cost savings in commercial software procurement can be accomplished through a check-in/check-out (CICO) system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	A PROLOGUE TO THE STUDY	1
B.	STATEMENT OF PURPOSE	1
C.	RESEARCH QUESTIONS	2
D.	SCOPE	2
E.	RESEARCH METHODOLOGY	3
F.	STUDY ORGANIZATION.....	3
II.	BACKGROUND ON COTS POLICIES AND PROCURMENT METHODS	5
A.	GOVERNMENT IT POLICIES, PRACTICES, AND DIRECTION.....	5
1.	The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)).....	5
2.	The DoD Enterprise Software Initiative (ESI)	6
3.	Changes in Acquisition Policies	7
4.	The Consolidation of Data Centers	9
5.	The Move to the Cloud	10
6.	Where are we Now?	12
B.	DOD COTS PROCUREMENT METHODS	13
1.	U.S. General Services Administration (GSA) Advantage.	13
2.	The National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) Government-Wide Acquisition Contract (GWAC).	15
3.	The Army Computer Hardware Enterprise Software and Solutions (CHESS)	15
III.	SWOT ANALYSIS OF A CICO SYSTEM.....	17
A.	STRENGTHS	17
1.	Funding	17
2.	Availability.....	17
B.	WEAKNESSES:.....	17
1.	Funding	17
2.	Availability.....	18
3.	Control	18
4.	Technical Considerations	18
C.	OPPORTUNITIES	19
1.	Sharing of Best Business Practices with Industry.....	19
2.	Eco-Friendly	19
D.	THREATS	19
1.	Security	19
IV.	FIEDLING OF A PILOT CICO SYSTEM.....	21
A.	OVERVIEW	21
B.	TESTING OBJECTIVES	23
C.	KEY FINDINGS AND RESULTS	24

V.	CONCLUSION, RECOMMENDATIONS, AND LESSONS LEARNED	27
A.	CONCLUSION	27
B.	RECOMMENDATIONS.....	29
C.	LESSONS LEARNED	31
	LIST OF REFERENCES.....	33
	INITIAL DISTRIBUTION LIST	35

LIST OF FIGURES

Figure 1.	The Metered Products Report	25
Figure 2.	Software Utilization Workflow.....	28
Figure 3.	DoD SAM Initiatives	30
Figure 4.	Automated Workflow Process Flow	31

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	GSA SWOT Analysis	14
Table 2.	ESI Mission & DoD Agreements	16
Table 3.	Check-In/Check-Out SWOT Analysis.....	20

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADT	Auto Discovery Tools
AFARS	Army Federal Acquisition Regulation Supplement
APC	Area Processing Centers
ATO	Approval To Operate
CECOM-LCMC	Communications-Electronics Command – Life Cycle Management Command
CHESS	Computer Hardware Enterprise Software and Solutions
CICO	Check-In/Check-Out
CIO	Chief Information Officer
CoN	Certificate of Networthiness
COTS	Commercial Off-the-Shelf
DISA	Defense Information Systems Agency
DoD	Department of Defense
DFARS	Defense Federal Acquisition Regulation Supplement
EE	Enterprise Email
EIM	Enterprise Infrastructure Management
ESLA	Enterprise Service Level Agreement
ESI	Enterprise Software Initiatives
FAR	Federal Acquisition Regulation
GNEC	Global Network Enterprise Construct
GSA	General Services Administration
GWAC	Government Wide Acquisition Contract
HQDA	Headquarter, Department of the Army
IaaS	Infrastructure as a Service
IPT	Integrated Product Team
IT	Information Technology
ITAM	Information Technology Asset Management
JAP	Joint Applied Project
JIE	Joint Information Environment

JCISA-P	Joint Command Information Systems Activity - Pacific
LWN	Land War Net
NASA	National Aeronautics and Space Administration
NETCOM	(U.S. Army) Network Enterprise Technology Command
OMB	Office Management and Budget
PEO EIS	Program Executive Office Enterprise Information Systems
PaaS	Platform as a Service
SaaS	Software as a Service
SAM	Software Asset Management
SMS	System Management Server
SEWP	Solutions for Enterprise Wide Procurement
SWOT (Analysis)	Strengths, Weaknesses, Opportunities, Threats
USDA	United States Department of Army

ACKNOWLEDGMENTS

We would like to thank our advisors, Mr. Brad Naegle, Professor Charles Pickar, and Professor Christina Kelton. This Joint Applied Project would never have happened without their energetic support. Thank you!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. A PROLOGUE TO THE STUDY

Over the years, there has been a great deal of computer software which Department of Defense (DoD) agencies have purchased that is never utilized. According to the U.S. Army Program Executive Office Enterprise Information Systems (PEO EIS), the DoD spends \$6 billion dollars a year on computer software (Wardle, 2011, p. 3) and it has increased 1,019 percent since the Clinger-Cohen Act of 1996 mandated the use of commercial specifications whenever possible. The United States federal budget deficit and the corresponding reduction in DoD spending has put constraints on our agencies to do more with less and cut back on all computer software expenditures. Budget cuts are making software assets highly visible to cost-conscious resource managers, forcing DoD information technology (IT) departments to streamline their vital inventories.

Currently, there are several DoD-wide and Component mandates or policies to consolidate the vast amount of homegrown data centers into large Area Processing Centers (APCs) with future sights set on Cloud Computing. One significant goal of this consolidation effort would be a great reduction in the amount of Commercial Off-the-Shelf (COTS) software being purchased by individual agencies. To further promote gaining efficiencies in IT, the Office of the Assistant Secretary of Defense, DoD CIO sponsors an Integrated Product Team (IPT) for Information Technology Asset Management (ITAM) to include members from all components of DoD.

B. STATEMENT OF PURPOSE

With the Department of Defense pushing more and more towards using COTS products, we will begin with an examination of the cost of commercial software usage in the DoD. Through an analysis of cost versus usage data, we propose that potential significant cost savings in commercial software procurement can be accomplished through a check-in/check-out system.

According to Frey (2005), the following can be said for the adoption of Commercial Off-the-Shelf acquisition practices.

There is a clearly discernible migration toward commercial off-the-shelf (COTS) procurement within the federal arena, particularly in the area of software products. COTS products represent industry's best—they are tested and piloted before deployment in the marketplace. They are also readily available off of the GSA schedule. Congress and the Office of Management and Budget (OMB) within the Executive Office of the President have indicated a preference for COTS solutions, which constitutes an important consideration in obtaining funding for a federal agency. (Frey, 2005, Chapter 3)

As the Department of Defense moves more towards the procurement of COTS, they will need a better way to procure, track, install, and manage what is purchased versus what is actually being used.

C. RESEARCH QUESTIONS

The purpose of this research is to determine if savings may be had in development of a check-in/check-out system for software. Below are the following research questions:

- What major processes do United States Defense Agencies (USDA) use to obtain/purchase COTS software?
- What are the potential strengths and weaknesses of an alternative check-in/check-out type of system?
- What are some examples of the difference between software purchased and software actually used?

D. SCOPE

This analysis will be conducted into four stages. The first phase begins with a review of current procurement process used by the United States Defense Agencies. We will examine pioneering DoD mandates such as the Clinger-Cohen Act of 1996, changes to the Federal Acquisition Regulation (FAR), and other statutory agreements that guide today's COTS procurements. The next phase presents a Strengths-Weaknesses-Opportunities-Threat (SWOT) analysis that was done on the potential strengths and weaknesses of an alternative check-in/check-out system for COTS procurement; a great deal of this research having been done via the Internet and books. The third phase looks at a pilot project that shows the difference between software purchased and software

actually used. The final phase looks at the results of all phases and provides lessons learned and recommendations for a check-in/check-out system.

Research material for the study was limited to on-line Internet sources, local bookstores, and public libraries. Supporting data was gleaned from a pilot project conducted at an Army installation.

The pilot project utilized an Asset Discovery Tool (ADT) that provided the relevant data needed to support decision workflows. The workflows dynamically suggested alternative actions from the real-time visibility of software assets. These suggested alternative actions that were based on, and adhered to, established Army and industry best practices for Software Asset Management (SAM) and Information Technology Asset Management (ITAM).

E. RESEARCH METHODOLOGY

Throughout this study we will look at the major processes that United States Defense Agencies (USDA) use to procure software, show examples of the difference between software purchased and software actually used, and present potential strengths and weakness of an alternative check-in/ check-out system. Through an analysis of cost versus usage data, we propose that potential significant cost savings in commercial software procurement can be accomplished through a check-in/check-out system.

F. STUDY ORGANIZATION

This study is comprised of five chapters.

Chapter I - Introduction

Chapter II – Background on COTS Policies and Procurement Methods

Chapter III – SWOT Analysis of a Check-In/Check-Out System

Chapter IV – Fielding of a Pilot Check-In/Check-Out System

Chapter V- Conclusions, Recommendations, and Lessons Learned

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND ON COTS POLICIES AND PROCURMENT METHODS

A. GOVERNMENT IT POLICIES, PRACTICES, AND DIRECTION

Founded in 1986, the Army Small Computer Program (ASCP) entered into the first DoD enterprise software agreement with Microsoft Corporation in 1995. This contract marked the first of many consolidated information technology (IT) procurements of COTS software that ASCP, later CHESS, would execute after the passage of the 1996 Clinger-Cohen Act mandated the use of commercial specifications whenever possible. This mandate formed the basis of government commercial software procurement, setting in motion a series of events and policies that are shaping DoD IT today. But how did the Clinger-Cohen Act have such long reaching effects? Let us take a look at the policy and its impact.

1. The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3))

The Information Technology Management Reform Act (ITMRA) (Division E) and the Federal Acquisition Reform Act (FARA) (Division D) were signed into law as part of the National Defense Authorization Act of 1996. Subsequently, the ITMRA and the FARA were designated the Clinger-Cohen Act (CCA) of 1996.

The ITMRA primarily established Chief Information Officers (CIOs) in government agencies with the goal of reforming and improving the process in which the Government acquired and managed its IT resources. The FARA supported the ITMRA by permitting the use of Simplified Acquisition Procedures in the acquisition of commercial items (CI) up to \$5 million.

With the establishment of Government CIOs and acquisition law reformed to facilitate the streamlined acquisition of CI, it wasn't before long that the DoD saw their component commands building up their own independent IT infrastructures using commercial items. Due to the lack of an over-arching DoD CIO level IT-roadmap at the time, agencies built up their own IT assets without consideration to potential savings and efficiencies that could be gained by standardized and centralized procurements.

2. The DoD Enterprise Software Initiative (ESI)

In the fall of 1998, DoD chief information officers (CIOs) met for the first time and established the DoD Enterprise Software Initiative (ESI) working group. These CIOs aimed to acquire and manage COTS as an enterprise IT resource, consolidate departmental requirements, and coordinate software acquisitions among the various DoD agencies.

Four core goals were established to guide the ESI mission:

- Obtain buy-in from DoD agencies for enterprise-wide software agreements.
- Reduce the acquisition and support costs of commercial software by leveraging DoD buying power.
- Provide the best, most flexible software suites of Joint Technical Architecture-conforming commercial software to the DoD Enterprise.
- Create a funding vehicle that promotes the use of DoD-wide software initiatives.

(Panaro, 2008, page-54)

Over a period 10-years (1998–2008), the DoD ESI has negotiated 75 enterprise software agreements with more than 50 software publishers, resulting in a \$3 billion cost avoidance for the DoD. So successful has the DoD ESI effort been that the Office of Management and Budget (OMB) launched a similar initiative for the rest of the federal government through the General Service Administration's (GSA's) SmartBUY initiative in the fall of 2003. There are now 22 ESI/SmartBUY co-branded agreements that allow all federal agencies to procure software. In 2007, this coverage was expanded to include state and local governments.

Flexibility, both in licensing agreements and funding methods, have also been a part of ESI licensing. Most ESI ESAs allow for licenses to be transferred between users of DoD components, and many permit transfers across the entire DoD. Additionally, there is a clause in most ESI agreements that provision for the right of an agency to surge the deployment of software in times of national emergency for a limited time and at no

additional cost to the government. This ability to easily transfer licensing and ramp-up deployment in contingencies complements the ESI's other key objective of central IT management.

In ESI's Information Technology Asset Management (ITAM) program, the DoD aims to use a net-centric, software-as-a-service model that would allow all IT assets to be pulled into a single repository. Through development of policy and guidance, the ITAM integrated product team (IPT) is building a net-centric framework that will incorporate all data about a components' IT assets, making them visible to DoD and federal government IT decision makers as a pool of common resources to draw from.

Thus with ESI, we can see the beginnings of a check-in/check-out (CICO) software system. Through the establishment and use of consolidated ESAs, the legal aspect of government-wide, cost effective, and flexible licensing of commercial software has been realized. The net-centric ITAM construct, once implemented, will provide the means to implement real-time, on-line IT asset management of those licenses. This ability to instantly assign and re-assign software licensing will make the software-as-a-service and software-on-demand features of a CICO software system achievable.

3. Changes in Acquisition Policies

With a DoD wide organization put in place to establish programmatic policies on IT asset management, parallel efforts in federal acquisition set in motion by the Clinger-Cohen Act eased procurement of commercial items. With the CCA-inspired addition to the Federal Acquisition Regulation (FAR) mandating the "acquisition of commercial or non-developmental items when they are available to meet the needs of the agency" (FAR, 2005, § 12.101(b)) , the Defense Federal Acquisition Regulation Supplement (DFARS) went further to align the acquisition of commercial software with the Enterprise Software Agreements (ESAs) established by the ESI.

Departments and agencies shall fulfill requirements for commercial software and related services, such as software maintenance, in accordance with the DoD Enterprise Software Initiative (ESI) (see Web site at <http://www.esi.mil>). ESI promotes the use of enterprise software agreements (ESAs) with contractors that allow DoD to obtain favorable

terms and pricing for commercial software and related services. ESI does not dictate the products or services to be acquired. (DFARS, § 208.7402)

With the rebranding of the Army Small Computer Program (ASCP) to the Army Computer Hardware, Enterprise Software, and Solutions (CHESS) Program in 2007, the Army mandated the use of CHESS as their primary source of COTS IT products in Army Regulation (AR) 25-1.

When an activity requires a COTS product, the supporting DOIM will determine if it is available from Computer Hardware, Enterprise Software and Solutions (CHESS), the Army's representative for the DOD Enterprise Software Initiative (ESI). (AR 25-1, § 6-2e(3))

By mandating the use of CHESS for its desktop and laptop computers, the Army also leveraged the labor force of CHESS suppliers by requiring vendors to pre-load their computers with the Army Golden Master (AGM). So much did the Army believe in the CHESS program's cost avoidance ability that the Chief Information Officer (CIO)/G6 issued a memorandum in May 2009 "to remind U.S. Army leaders of the existing requirement to use CHESS for purchases of commercial off-the-shelf (COTS) software, desktops, notebook computers and video teleconferencing equipment, regardless of the dollar value" (DA CIO/G6, 2009, p. 1). Additionally, by procuring their computers through CHESS, Army users could ensure that their computers would arrive from the vendor, ready to deploy, loaded with the Army's standard desktop/laptop baseline software configuration. The AGM software build, which consisted primarily of the ESA-licensed Microsoft Windows operating system and Office productivity suite, also had the added benefit meeting mandated Federal Desktop Core Configuration (FDCC) security requirements¹.

To further ease the influx of COTS products into the DoD, the Federal Acquisition Regulation was revised in 2009 to include a list of "provisions of law that are inapplicable to contracts for the acquisition of commercially available off-the-shelf (COTS) items". (Federal Register, 2009, p. 2713)

¹ FDCC has been superseded by the United States Government Configuration Baseline (UCGCB) security initiative maintained by the National Institute of Standards and Technology (NIST).

COTS items are defined in 2.101. Unless indicated otherwise, all of the policies that apply to commercial items also apply to COTS. Section 12.505 lists the laws that are not applicable to COTS (in addition to 12.503 and 12.504) ; the components test of the Buy American Act, and the two recovered materials certifications in Subpart 23.4, do not apply to COTS. (FAR § 12.103)

It was inevitable that such regulatory reforms coupled with the flexible volume licensing provided by ESI's ELAs, and applicability of Simplified Acquisition Procedures would result in a plethora of DoD COTS IT purchases. However, in today's bleak DoD spending environment, this uncoordinated collection of IT assets is unsupportable; a collection of overlapping and often redundant systems.

4. The Consolidation of Data Centers

In May 2011, Headquarters Department of the Army (HQDA), issued an Execute Order (EXORD) for a 75% reduction goal in all Army Data Centers by Fiscal Year (FY) 2015. The goal of this EXORD, known as the Army Data Center Consolidation Plan (ADCCP), was to "gain efficiencies, improve performance, and increase security" (HQDA, 2011, p. 5). This policy follows OMB's earlier 2010 Federal Data Center Consolidation Initiative (FDCCI) and is in line with the forthcoming DoD IT Consolidation Roadmap.

One notable EXORD quote, centering on the Army's software inventory, addresses the need for software asset management. This need could be fulfilled by the proposed CICO system.

1.E. (U) THE ARMY'S SOFTWARE APPLICATION INVENTORY IS UNAFFORDABLE, DIFFICULT TO SECURE, AND CONTAINS REDUNDANT/LEGACY APPLICATIONS. APPLICATION MIGRATION HAS PROVEN VERY CHALLENGING AND IS THE PACING ITEM FOR THE ADCCP. (HQDA, 2011, p. 4)

Following the issue of the ADCCP EXORD, HQDA CIO/G6 issued its third memorandum on its "Moratorium on IT Spending" in December 2011. This memorandum expanded on the previous 2010 ban on the procurement of servers and

voice switching equipment to include construction, renovation and/or leasing of data centers or server rooms, and procurement of IT equipment which would be utilized in a data center or server room. Any command with an urgent requirement to invest in an Army data center would have to submit a waiver to HQDA, CIO/G6 before pursuing with the acquisition.

5. The Move to the Cloud

In July 2012, the DoD Chief Information Officer, Ms. Teresa M. Takai, announced the agency's long-term vision of the move to cloud computing. Driving this initiative is a target information infrastructure known as the Joint Information Environment, or JIE.

The Joint Information Environment is a robust and resilient enterprise that delivers faster, better informed collaboration, and decisions enabled by secure, seamless access to information regardless of computing device or location. The DoD Enterprise Cloud Environment is a key component to enable the Department of to achieve JIE goals. (DoD CIO, 2011, p. E-1)

The DoD Enterprise Cloud Environment will include implementation and data exchanges on the three predominant classifications of DoD networks: the Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRNET), the Secret Internet Protocol Router Network (SIPRNET), and Top Secret Sensitive Compartmentalized Information (TS SCI) security domains.

Each Cloud Environment will establish an Enterprise Cloud Service Broker to manage the use, performance, and synchronized delivery of cloud services to the end-user. This brokerage service is conceptually the same as a virtual librarian "agent" in the proposed check-in/check-out (CICO) system. The service, or software agent, would act on behalf of the user to determine if requested services, such as a licensed copy of a COTS application, were available from the DoD-wide pool of IT resources to "check-out". Benefits to be gained out of "commoditized" cloud services include such CICO features as pay-as-you-go pricing for services on-demand, and flexible scalability to support surge users as mission needs grow.

To get the DoD Enterprise Cloud Environment, the Department has identified four concurrent steps that will be implemented:

1. Foster the Adoption of Cloud Computing
2. Optimize Data Center Consolidation
3. Establish DoD Cloud Infrastructure
4. Deliver Cloud Services

From early net-centric concepts such as the Global Information Grid (GIG), the Navy's Navy Marine Corps Intranet (NMCI), the Air Force's Combat Information Transport System (CITS), and the Army's Land War Net (LWN), the focus to build the Joint Information Environment made Cloud Computing an integral part of every DoD IT infrastructure project.

With Data Center Consolidation efforts underway at the Federal, DoD and Component levels, the basic Cloud Computing service model of Infrastructure as a Service (IaaS) will soon be realized.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (DoD CIO, 2011, p. C-2)

As the Consolidated Data Centers stabilize and users transition off of legacy networks and local application, we will see the establishment of the early DoD Cloud Infrastructure. This pre-JIE environment would be the fielding ground for the proposed CICO software system; a DoD-wide repository of COTS software titles with a limited-duty software agent "librarian" checking available titles against "borrower" requests. Finally, moving toward the delivery of full Cloud Services, we will see the transition of the Cloud Computing service model from IaaS to SaaS, or Software as a Service.

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a

thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (DoD CIO, 2011, p. C-1)

In this end-state-environment, our CICO software “librarian” will have expanded its duties from checking-in and checking-out locally managed software titles to a fully-fledged Cloud Service Broker, a “concierge” responsible for managing the use, performance, and synchronized delivery of all cloud services being offered.

Finally, to reinforce this overarching IT-architecture directive towards cloud computing, the federal government has passed laws addressing future investments in data servers and centers in the National Defense Authorization Act (NDAA) for Fiscal Year 2012. Through this enactment, it became unlawful after May 1, 2012 for a department, agency, or component of the DoD to obligate funds for a data server farm or data server unless approved of by the DoD CIO, or a component CIO delegated the authority by the DoD CIO.

Furthermore, the 2012 NDAA required the DoD CIO to establish a defense-wide performance plan to reduce the amount of resources required for data centers and information systems technologies. Among other things, such as green technologies for power and cooling, this plan called out for DoD to put in place strategies to transition to cloud computing; to migrate defense data and government-provided service from DoD-owned and operated data centers to commercial cloud computing services at lower cost and equal or greater security; and to utilize private sector managed security services for cloud computing services.

6. Where are we Now?

As of August 21, 2012, the Army has taken its first step toward utilizing DoD Enterprise Cloud Services having transitioned half-a-million NIPRNET email accounts from locally managed Microsoft Exchange servers at all of its worldwide installations to the centrally managed, DISA-sponsored, Enterprise Email system (Bailey, 2012).

B. DOD COTS PROCUREMENT METHODS

With the way forward to the future of government cloud computing defined by IT policies and procurement laws, let us take a look at the major processes that United States Defense Agencies (USDA) use to obtain/purchase software today

1. U.S. General Services Administration (GSA) Advantage.

GSA Advantage is a government purchasing service of the General Services Administration. It was created in 1949 as an independent agency of the United States government established to help manage and support the basic functioning of federal agencies. GSA Advantage is an online purchasing service created by the GSA organization. Its mission is to provide a streamlined, efficient purchasing portal for federal agencies to acquire the goods and services needed.

GSA was created with three goals in mind. First, it was created to reduce the time, cost, and bureaucracy involved in purchasing goods and services. Second, GSA was to secure the lowest possible price available for the federal government customer. Third, and most importantly, GSA was mandated to verify that contractors are qualified to sell to the federal government.

Table 1. GSA SWOT Analysis

Internal	
Strengths	Weaknesses
<ul style="list-style-type: none"> • Time frame to procure software is significantly reduce • Avoid the competitive process • Price can still be negotiated 	<ul style="list-style-type: none"> • Pre-negotiated pricing and terms and condition • Reduced control over responsiveness when negotiating • Bureaucracy
External	
Opportunities	Threats
<ul style="list-style-type: none"> • Communication between government and customers • Technology changes • Resources and Partner 	<ul style="list-style-type: none"> • Security from abroad • Legislation • Resources unfunded mandates • Enterprise approach
SWOT Analysis Summary	
<p>Advantage and disadvantages of GSA schedule GSA's Federal Supply Schedule makes it easier for Department of Defense Agency to buy Commercial-of-the-Shelf software. GSA has contracts with commercial firms to provide various products and services to DOD agencies. The procurement procedure has been streamlined where rates have been negotiated, and vendors have been prequalified by the government. DOD agencies can procure products from contractors on the GSA schedule.</p>	

2. The National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) Government-Wide Acquisition Contract (GWAC).

NASA SEWP is a GWAC authorized by the U.S. Office of Management and Budget (OMB) and managed by NASA. NASA SEWP provides a wide-array of Information Technology (IT) products as well as product related services such as installation, implementation, warranty, and maintenance. All Federal agencies including the Department of Defense are able to purchase from NASA SEWP.

3. The Army Computer Hardware Enterprise Software and Solutions (CHESS)


Army CHESS, is a program managed under the Program Executive Office, Enterprise Information Systems (PEO EIS). CHESS is the Army's mandated primary source for commercial Information Technology (IT); providing a no-fee, flexible procurement strategy through which an Army user may procure commercial-off-the-shelf (COTS) IT hardware, software, and services via an e-commerce based process called "T e-mart". These contract vehicles provide continuous vendor competition for best value and consolidation of requirements to maximize cost avoidance and leverage the Army's buying power.

DoD Enterprise Software Initiative was established June 1998 by the Chief Information Officers at the DoD, to lower cost and save money on commercial-off-the-shelf software across the enterprise. ESI provides valued returns on investments on COTS to individual services and agencies otherwise not available.

Enterprise Service Level Agreements (ESLA) is designed to manage and perk up conventional levels connecting IT providers and customers. This promotes both parties getting together and coming up with a joint resolution to produce large software discounts.

The Enterprise Software Initiative statement and a selection of current DoD ESI agreements are shown in Table 2

Table 2. ESI Mission & DoD Agreements

 <div> ENTERPRISE SOFTWARE INITIATIVE </div> <div>ESI Pricing</div>
<p>The DoD ESI is a joint project designed to implement a software enterprise management process within DoD. By pooling our current and future requirements for commercial software and presenting a single negotiating position to leading software vendors, DoD ESI provides pricing advantages not otherwise available to individual Services and Agencies. Twenty three software best practices have been identified and adopted by the DoD ESI Working Group, leading toward a DoD-wide business process for acquiring, distributing and managing enterprise software. Agreement negotiations and retail contracting actions are performed by IT acquisition and contracting professionals within participating DoD Services and Agencies, as DoD ESI "Software Product Managers". For more detailed information visit the DoD ESI at http://www.esi.mil. DoD ESI also offers selected IT services and is implementing IT Asset Management across DoD with linkages to the DoD Component level. The DoD ESI Team promotes regular sharing of information about DoD Component IT hardware enterprise acquisition practices, and is represented on DoD's Strategic Sourcing Board of Directors, and on the Federal Strategic Sourcing Initiative's IT Commodity Team.</p>
CURRENT DoD ESI AGREEMENTS (SAMPLE SET)
<p>Adobe Desktop and Server software at up to 60% off GSA TLP level 1 pricing.</p>
<p>Autodesk Included in this award are over two dozen AutoCAD and Autodesk products, at a discount of up to 10% off of the GSA price.</p>
<p>CA Unicenter enterprise management software is available at 64% off; <i>BPwin and Erwin</i> modeling tools (including product, maintenance, and upgrades) are available at 56% off GSA FSS prices.</p>
<p>IBM's five newly established "product lines" – Rational, DB2, Tivoli, Lotus and Websphere – and IBM/Informix DB software are available at up to 27% off GSA FSS pricing. Rational Enterprise Architecture Software and maintenance discounts up to 14% of GSA FSS.</p>
<p>Microsoft's software products for desktop configurations, servers and other products at up to 38% off GSA FSS pricing by nine resellers.</p>
<p>Microsoft Premier Support Services provided at 4% off list price volume of transactional buy; greater reductions available through spot discounting.</p>
<p>NetIQ systems & security management /web analytic tools are discounted at up to 18% off GSA FSS.</p>
<p>McAfee and Symantec anti-virus products are available at no cost. (See JTF-GNO Web site: https://patches.csd.disa.mil/Default.aspx for free downloads.)</p>
<p>McAfee (Securify) Network Security Management System and other products and services at 4% to 36% off GSA Schedule prices</p>
<p>Red Hat Linux operating systems software and services at 10% to 48% off GSA FSS price.</p>
<p>SAP Enterprise Resource Planning software starting at 33% off GSA FSS prices. Greater discounts are available for higher volume.</p>
<p>Sun Software Supplies integration and service oriented architecture SOA software. SUN Java Enterprise Systems (JES) includes JES Identity Management Suite, JES Communications Suite, JES Availability Suite and other SUN JES products at 10% off GSA FSS prices.</p>

III. SWOT ANALYSIS OF A CICO SYSTEM

This next phase of our research examines the potential strengths, weaknesses, opportunities, and threats (SWOT) of an alternative check-in/check-out type system. We start our analysis with the scenario of an organization's annual purchasing of COTS software then move the potential benefits and risks of a CICO system

A. STRENGTHS

1. Funding

- a) Cost savings in COTS software due to elimination of “stock-piling” of unused software licenses.
- b) Elimination/reduction of software upgrade costs. Through leasing of software, users get the next version as it is released and added to the “borrow pool”.

2. Availability

- a) Maximizing use of a software license. When a user no longer needs a piece of software, he/she returns the license it to the “library” for others to use.
- b) Reduction in physical media & storage requirements. By having a check-in/check-out system, Information Technology (IT) Operations & Maintenance (O&M) personnel no longer have to account for, maintain, and store multiple physical copies of COTS software. Software will always be available for download.

B. WEAKNESSES:

1. Funding

- a) Software lease payments, if timed with fiscal year funding, may add considerable year-end workload to existing government COTS contract offices.

- b) In the current austere fiscal environment, delays in 1st quarter fiscal year (FY) funding may cause lapses in software licensing, software expiration, and eventually loss of user capability.

2. Availability

- a) Software license may be unavailable for “check-out” if the maximum authorized number of copies is exceeded. As an analogy, think of the library patron attempting to borrow a book, only to find that it is overdue; not returned on-time by another patron.

3. Control

- a) Most widely deployed COTS products, such as Microsoft Office, are licensed to the DoD under site licensing for an estimated amount of users. While a command is required to have a license to install and use a site-licensed COTS product, there is no apparent built-in mechanism to automatically track and control the number of actual users utilizing a site license. If the check-in/check-out system does not address the problems of site-license misuse the software vendor will not be fairly compensated.

4. Technical Considerations

- a) With software constantly being “checked-in” and “checked-out” from a central repository, what is the impact on network bandwidth utilization to support the associated increase in software downloads and license verification? This is of particular concern to forward-deployed military units where network connectivity is limited.
- b) Applicability in Wartime (or Deployed) Environment. Can a check-in/check-out system be successfully deployed and utilized in an operational environment where network resources are limited and network security heightened? If software vendors maintain the

“software libraries”, are they able to support COTS users on classified networks?

C. OPPORTUNITIES

1. Sharing of Best Business Practices with Industry

- a) Government will leverage off of lessons-learned from Industry in deploying cloud computing services such as CICO. While the government is in its infancy in deploying CICO technology, commercial IT industry leaders, such as Amazon and Apple, have been loaning out software titles, albeit video titles, for several years through their on-line commerce sites.

2. Eco-Friendly

- a) Less physical copies of software and associated documentation will be more environmentally friendly; less CDs/DVSs, less plastic CD/DVD covers, less cardboard packaging, and less paper manuals.

D. THREATS

1. Security

- a) Virus infected copies of S/W could have DoD wide effects. If the CICO software repository were to become infected with a virus or other malware, the virus would easily be transmitted whenever the software is loaned out to a borrower. (This problem is not inherent with purchases of individual software packages from different vendors unless the virus is present on the software publishers release.)
- b) Once compromised with a virus, a CICO system could be used a launch site for cyber-attacks against other trusted systems and their networks.

Table 3. Check-In/Check-Out SWOT Analysis

Internal	
Strengths	Weaknesses
<ul style="list-style-type: none"> • Cost Savings – No “Stockpiles” • Eliminate/Reduce H/W & S/W upgrade costs • Maximize use of S/W licenses • Reduction in storage space for physical media 	<ul style="list-style-type: none"> • Additional workload for contracting commands on year-end lease renewals • Lapses in S/W licensing due to late availability of 1Q FY funding • Unavailability of S/W due to limits on licensed copies • Monitoring and control of number of S/W licenses authorized for use • Availability of network bandwidth to support CICO system • Applicability in “wartime” environments and classified networks
External	
Opportunities	Threats
<ul style="list-style-type: none"> • Sharing of best business practices between government and industry • Environmentally friendly S/W deployment model 	<ul style="list-style-type: none"> • Virus infected software has the potential to contaminate all clients using the CICO system. • CICO system could be used as a launch point for a cyber-attack.
SWOT Analysis Summary	
<p>As in all IT-related initiatives there are weaknesses and threats that must be overcome to implement a Check-In/Check-Out (CICO) system. However, with such benefits as reduction in software licensing costs, smaller physical footprint needed for storage, and being more eco-friendly, the move toward CICO is a natural progression toward the government’s and DoD’s cloud-based computing initiative</p>	

IV. FIEDLING OF A PILOT CICO SYSTEM

A. OVERVIEW

Now that we've touched upon governmental policies and regulations, and conducted an analysis of the pros and cons of a Check-in/Check-out system, can we determine the difference between software purchased and software actually used in a DoD environment? This question was the basis of the Check-in/Check-out pilot project.

Initiated in March of 2007, the pilot project aimed to realize reductions in the cost of software licensing and maintenance, provide better control over the existing Army Commercial-off-the-Shelf (COTS) software inventory, and gain efficiencies in the procurement of future software assets, within the Enterprise Infrastructure Management (EIM) of the Army.

According to an article in CHIPS magazine by Chris Panaro titled, "DoD ESI Celebrates its 10th Anniversary.", more than 3 billion dollars in cost avoidance was achieved by ESI in the first decade.

When the Department of Defense Enterprise Software Initiative (ESI) working group met for the first time in the fall of 1998, little did they know that 10 years later they would be responsible for more than \$3 billion in cost avoidance for the DoD. In acknowledgment of its 10th anniversary, the ESI working group went back to some of those early ESI visionaries and some current users to get their thoughts on the initiative over the years. ESI began as a collaborative effort among the DoD chief information officers (CIOs), but it has turned into an award-winning, DoD-wide initiative with more than 75 enterprise software agreements (ESAs) with more than 50 software publishers for thousands of software products and services. "ESI changed how the entire department acquires and licenses commercial software," said Dave Wennergren, Deputy CIO for DoD. "Without ESI, we would never have leveraged our buying power, understood our department-wide requirements, significantly

reduced the labor required to manage software licenses, or have achieved the dramatic reduction in costs of several billion dollars. I applaud the ESI team for its success and contributions over the past 10 years.”² (C. Panaro 2008, p. 1)

Microsoft Systems Management Server (SMS) 2003 was used at this Army location as the Auto Discovery Tool (ADT) for managing hardware inventory, software inventory, software distribution, and remote client troubleshooting. The Army, in conjunction with a vendor and Enterprise Infrastructure Management (EIM) practices, selected the use of SMS as the ADT of choice for the pilot. This selection was made for several reasons:

1. SMS was already licensed by the Department of the Army under an Enterprise Service License Agreement (ESLA).
2. SMS was distributed on the Army Gold Master software release for its desktop computer and server environment.
3. SMS could be maintained at all Army facilities and controlled by individual organizations.

It should be noted that although testing was limited to using strictly Microsoft SMS, most commercial Auto Discovery Tools (ADT) could also have been used to conduct the pilot. There were 54 test cases which were manually executed multiple times in order to evaluate how the proposed check-in/check-out pilot system would perform in the following 6 key areas of:

1. System Functionality – Is the system functioning as it was designed. Do all the links, images, exists and are they displayed correctly. Is the navigation working correctly? Is the system able to provide the necessary information to support knowledge-based decisions regarding the request, the reassignment and/or the retirement of software licenses and renewal of maintenance support services?
2. System Integration - How are the interactions between browsers and servers, applications, data, software and hardware functioning? Does the system

provide for continuous feed and seamless blend into a central repository of auto discovery data from across the Army?

3. System Security System Usability - Are the security controls for User access and authorization working?
4. System Reliability Outages – How reliable is the system? Does the system provide consistent and correct results? Is the system available on a consistent basis?
5. System Documentation - How does the documentation measure up? Does it provide the necessary information? Does it provide enough information?
6. System Performance. - During execution of the test cases, system performance was evaluated but only from a User's perspective. In other words, how a typical User might expect the system to perform. The focus was on User wait times during login, navigation, screen refresh, edits, saves, reports, etc. and not on measured system response times.

B. TESTING OBJECTIVES

The overall objective of the test was to generate the requisite information needed to facilitate an automated decision process, derived from ADTs and the databases of raw data captured. These data sources were fed into the Repository. The army organization acquired the initial inventory of installed software on its domain to establish a baseline. Next, it established a list of COTS then cataloged and searched the baseline inventory for the unique executable files relative to the COTS. The results identified 20 of 28 COTS packages, “metered COTS”, as the most popular applications acquired by organization. The organization identified all existing procurement information and COTS licenses found in their database, and then matched them to relative metered COTS. The organization migrated the procurement and license information from a flat comma-separated-variables (CSV) file into the Repository. The data was then de-conflicted, analyzed, organized, and used to populate reports identifying the appropriate Decision Workflow to be used by management. The decision workflow was used to determine

whether additional licenses should be acquired, transferred to another Army organization for reuse, or kept in-house inventory. These findings provided the licensing solutions that applied to the needs of the organization, depicted volume license availability, and provided cost avoidance and savings associated with license fees and maintenance costs. Figure 1 describes the pilot process, identification of applications to be metered, then compares their metered results against data from appropriate authoritative source

C. KEY FINDINGS AND RESULTS

The findings in the System User Report indicated that these metered COTS products were frequently being left on overnight. This report identified the system user, usage summaries per user, and the user's workstation at the organization. Five users were flagged for high application usage of more than 20,000 minutes per month. Each row in the report represented an active session and was a summary of multiple usages. What this means is that 20,000+ minutes of application usage did not have to be in one continuous session. Still, 20,000 minutes is equivalent to 13.8 days, or close to 2 weeks, of usage.

There is no conclusive licensing data for the individual Microsoft products at this time. Several problems were quickly identified with metering COTS purchased through the ESLA. The ESLA offered bundled discount prices based on multi-year contracts. Microsoft Office 2000 included 6 core applications while Microsoft Office 2003 included 7 core applications. Microsoft Office Enterprise 2007 increased its core applications to 10, while Microsoft Office Professional 2007 just included 6. For those agencies that didn't need "Enterprise" but needed more than "Professional", Microsoft offered its Office Professional Plus 2007 which included 8 core applications. Since licensing information is stored differently for each Office Suite for Microsoft Volume Licenses, no one-to-one relationship currently exists between the core Microsoft products, product bundles, the individual applications, and price.

The Metered Products Report provided an accurate status on the COTS found on the pilot programs tested workstations. This report lists all metered products and the executable file name for each metered product. (Descriptions of additional reports are in

the section called Report Descriptions.) The Imported License report revealed that the organization had 275 copies of Corel WinZip 11.1 Standard License at a Total Cost of \$2,191.75 (\$6.75/unit); comprised of a Total License Cost of \$1,856.25, and a Total Maintenance Cost of \$335.50 (\$1.22 /unit). The analytical Software License Utilization Report indicated that there were 203 WinZip License available for use at organization, out of the 275 owned. By reassigning or deleting these licenses, the organization would have a yearly savings of \$1,617.91. This report also showed that the organization was using 35 licenses for Adobe Acrobat Professional that they did not own. It would cost the organization \$5,569.20 to be legally compliant with licenses.

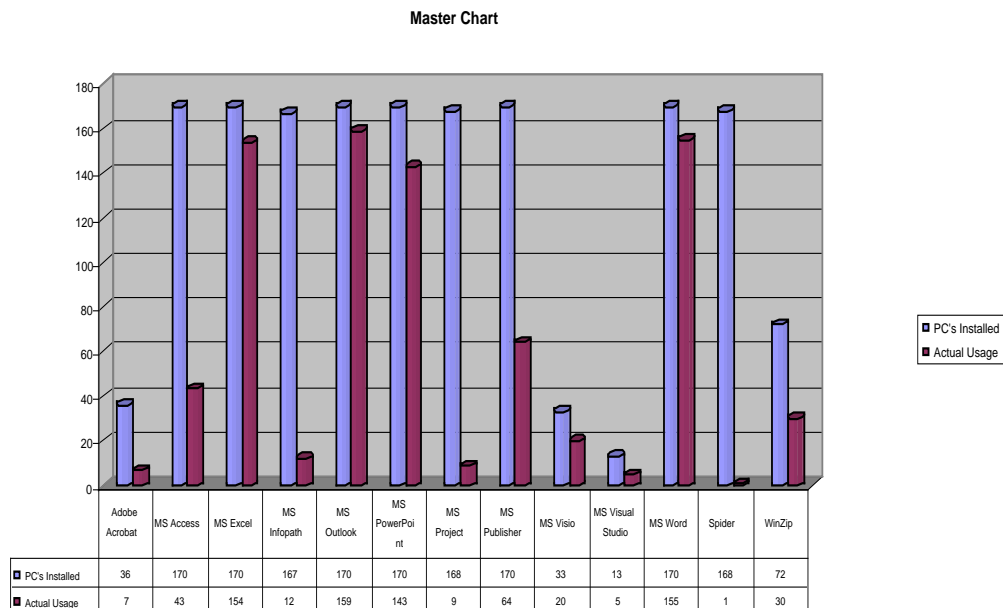


Figure 1. The Metered Products Report

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION, RECOMMENDATIONS, AND LESSONS LEARNED

A. CONCLUSION

The pilot proof-of-concept was a success. Testing confirmed that a seamless blend of data from across the army could indeed be achieved through a continuous feed of data from selected auto discovery tools (ADTs). The pilot team developed reports, then gathered information from the organizations combined data sources to populate those reports. Data points addressed included tracking software licenses that were not assigned, tracking licenses that were used in violation of the quantity on hand, workstation assignment by user, and identification of application usage.

In addition, the pilot team was able to demonstrate cost savings and cost avoidances associated with the Army organization's data. Several Decision Workflows were developed and are available for use for Proof of Concept trials by other agencies. The supporting information needed by the Decision Workflows was captured and reports were generated to address licenses that were not assigned, licenses that were used in violation of the quantity on hand, workstation assignment by user, and which applications were being used the most.

The findings identified a COTS solution that applied to the needs of organization; depicting volume license availability, cost avoidance, and savings associated with license fees and maintenance costs. The following reports show valuable asset information which, if implement throughout DoD, have the potential to provide savings in cost and cost avoidance.

- The **Metered Product Report**, shows a list of all metered products and the executable file name for each metered product.
- The **Organization Imported License Report** shows the licenses data for software products which has been imported from the database to the repository. It shows the Software Product Name, Maintenance Start Date, Expiration Date, Quantity, Total Cost, Unit Cost for license, Total Cost for license, unit Cost for maintenance and Total Cost for maintenance for the product.

- The **Software License Utilization Report** shows the data on licenses for software products. It shows the Software Product Name, the number of Systems with the Product, the number of Systems Using the Product, Licenses Owned, Licenses Available, Unit Cost, the Cost Differential and the Applicable Workflow. In Figure 2, the Utilization Report facilitates Decision Making through the visibility of total enterprise vulnerability, lifecycle requirements, and costs utilizing workflows.

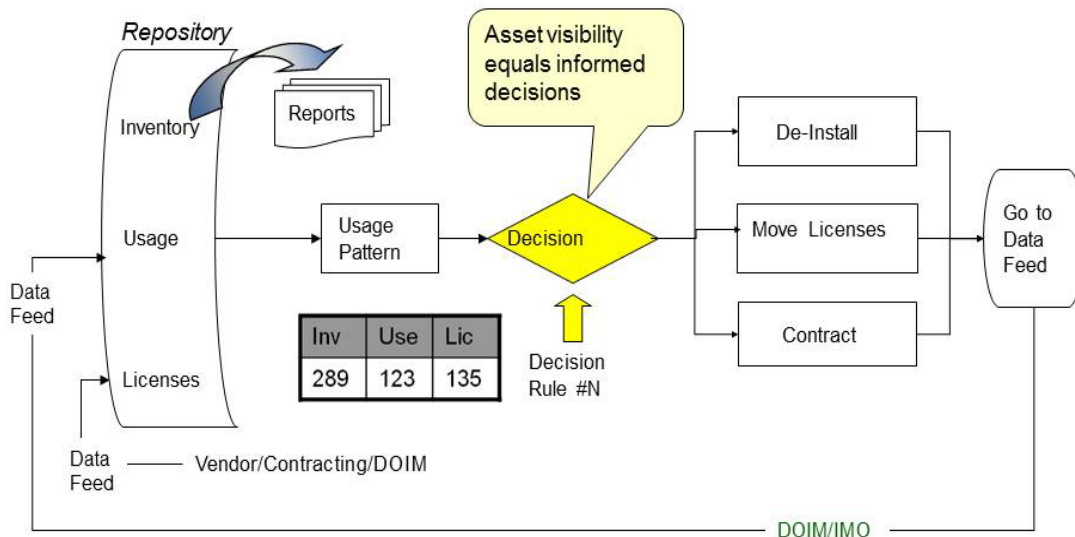


Figure 2. Software Utilization Workflow

- The **System User Report** shows the use of software for a system and a user for specified interval. It shows the System Name, Product Name, User Domain/Name, Usage Time in minutes, number of Usages and the selected intervals.

With the total of Army software inventory data, this research has identified the means in which the DoD and the Army enterprise software initiatives can better: identify and prioritize candidates for enterprise consideration; scope requirements for enterprise software agreements; maximize savings based on the total Army volume ordering; and determine best value licensing alternatives to meet Army needs. The Enterprise pays for no more and no fewer COTS licenses than are needed, and software is acquired and maintained at the most efficient cost per license.

B. RECOMMENDATIONS

With the proper Army Information Technology Asset Discovery Tool Program Implementation, commanders at all levels will have more complete and accurate information to assist in ensuring the security and integrity of the Army IT assets connected to the Army's LandWarNet (LWN).

Future plans should include capturing multiple DoD sites data, receiving data from the additional sites, standardizing data and product names, building required ADT interfaces, and automating additional workflows. The continued collaboration with the DoD community is critical in developing standards and policies to govern future methodologies. DoD should take an initial inventory of installed software on its domain, then organize and analyze the results to compare the combined software inventory against license information. As shown in the pilot, cost avoidance and savings achieved through centralized software support significantly offsets the manpower cost for providing these services.

Thus, the implementation of a check-in/check-out system could maximize cost avoidance and inventory utilization, reduce software procurement costs, increase COTS reuse through a total asset visibility, improve compliance with IT procurement policies, streamline and standardize the procurement process, and pre-position agencies for emerging DoD mandates and supporting DoD Enterprise Software Initiatives.

Through optimization of multiple portfolios established by Army projects, the DoD can impact how pilots influences the purchasing, tracking, transferring, stocking, and renewing of COTS licenses and maintenance agreements. This focus would include tracking assets from the conception to termination of the software life cycle. For example, a National Inventory Control Point for COTS software could be established, creating centralized capabilities for re-use, buy point determination, maintenance and disposal.

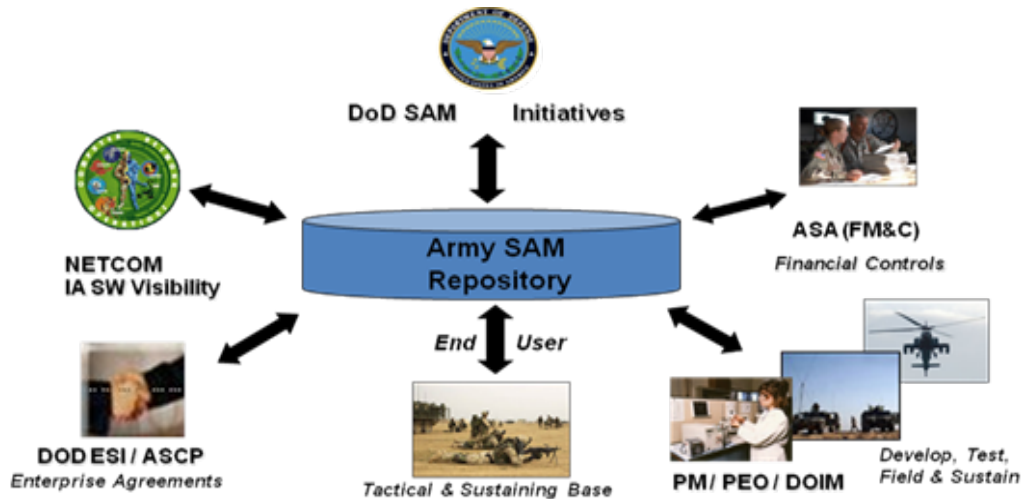


Figure 3. DoD SAM Initiatives

DoD should work with Industry to identify its most used COTS products, in order to influence the configuration of selected ESLA COTS product bundles. Identification of COTS files will aid in developing a fingerprint catalogue required for tracking and metering of COTS by executable files. The next step would be to determine authoritative sources, data elements, standards and descriptors required to support licensing, maintenance, contractual and financial data requirements associated with software assets tracked in the central repository. Finally DoD must support objectives for the continuous feed and seamless blend of data points into a central repository of auto discovery data across DoD and validate the methodology for implementing an ongoing SAM plan. A sample diagram of an automated workflow is shown below.

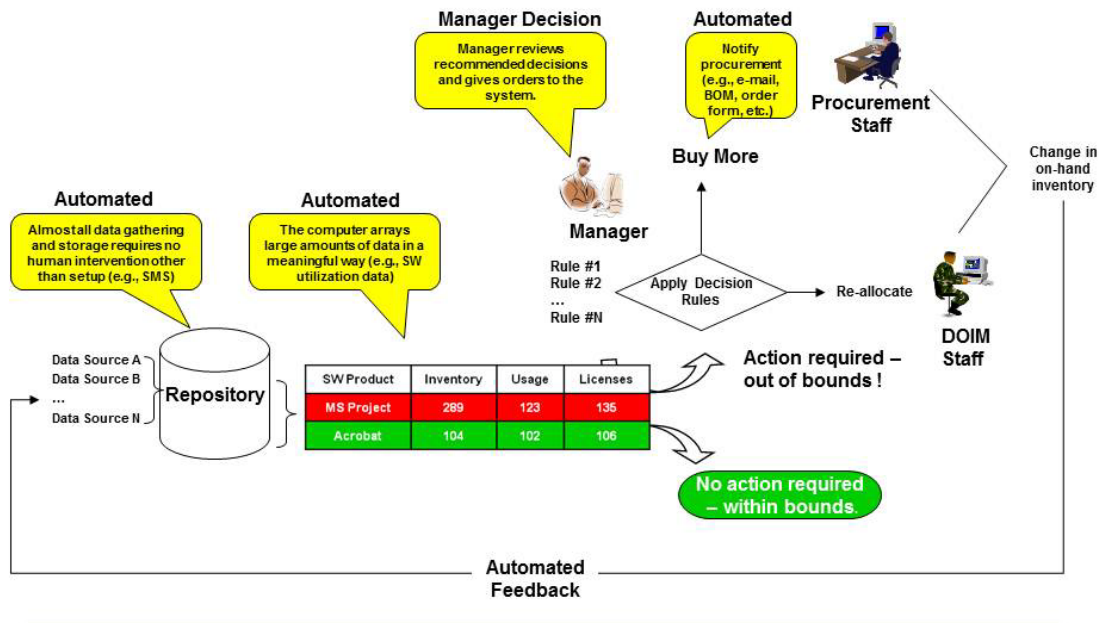


Figure 4. Automated Workflow Process Flow

C. LESSONS LEARNED

Throughout the deployment of the pilot CICO system, there were several unanticipated obstacles that were overcome or addressed. These issues ranged from DoD accreditation policies for deployment of COTS software to the security settings on the current Army Gold Master (AGM). These lessons learned should be noted and incorporated into future deployments of Check-In/Check-Out systems throughout DoD.

As we first deployed the pilot system, there were changes to the DoD Information Assurance Certification and Accreditation Process (DIACAP), which mandated new requirements for active network ports. Each time the requested ports changed, the DIACAP had to be resubmitted for approval. Port Activation requests for ports to be opened delayed the project extensively. This impacted the Authority to Operate (ATO), defined as a formal declaration by a Designed Approving Authority (DAA) to authorize operation of a Business Product on the network and explicitly accept the risk to agency operations. The ATO is signed after a Certification Agent (CA) certifies that a system has met and passed all requirements to become operational. This process delayed the

pilot for a year but could have been averted by just identifying persons and/or organizations that could have authorized Firewall Port Activation (FPA) request.

Next, the Army Gold Master Disk (AGM) security settings severely impacted our SMS surveying capability around which the pilot system was based. SMS Advance Clients did not work properly with the default AGM security configuration; a configuration which is replicated and distributed Army wide. CHESS should be notified to adjust their AGM configuration to support SMS client interrogation. If not resolved, this issue will encourage AGM non-compliance for SMS Servers.

Lastly, a number of applications have already been granted the U.S. Army Network Enterprise Technology Command's Certification of "Networthiness" (CoN) and/or Approval to Operate (ATO) while the majority of others have not. Expenses for testing and certification, therefore, need to be projected for every fielded application from performing simple reviews to conducting thorough checks on what work has been done on getting a CoN or ATO put in place for software in question.

LIST OF REFERENCES

- Bailey, B. (2012, August). *Half-million Army accounts migrated to Enterprise Email*. Retrieved from <http://www.army.mil>
- Carey, R. (2012, July 12). *Q&A: Rob Carey on the Joint Information Environment* (Interview by D. Perera) [Blog post]. Retrieved from Fierce Government IT website: <http://www.fiercегovernmentit.com/story/qa-rob-carey-joint-information-environment/2012-07-12>
- Chief Information Officer, Department of Defense (DoD CIO), (2012, July). *Cloud Computing Strategy* [Report] (T. M. Takai, Author). Retrieved from <http://dodcio.defense.gov>
- Chief Information Officer/G6, Department of the Army (DA CIO/G6), (2009, May). *Use of Computer Hardware, Enterprise Software and Solutions (CHESS) as the Primary Source for Procuring Commercial Information Technology (IT) Hardware and Software* [Memorandum].
- Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. ch. 2 (2011).
- Federal Acquisition Reform Act (FARA) of 1996, 40 U.S.C. § 104-106, Division D. (1996).
- Federal Acquisition Regulation (FAR), 48 C.F.R. ch. 1 (2005).
- Federal Register (FR). (2009, January 15). *Rules and Regulations*. Retrieved from <http://www.gpoaccess.gov/fr/index.html>
- Frey, R. S. (2005). *Successful Proposal Strategies for Small Businesses (4th ed.)*. Norwood, MA: Artech House Technology Management and Professional Development.
- Headquarters, Department of the Army (HQDA), (2011, May). *ALARACT HQDA Execute Order (EXORD) 209-11, Army Data Center Consolidation Plan (ADCCP)*.

Information Technology Management Reform Act (ITMRA) of 1996, 40 U.S.C. § 104-106, Division E (1996).

National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, 112th Cong., 1st Sess. § 2867 (2012) (enacted).

Panaro, C. (2008, December). *DoD ESI Celebrates its 10th Anniversary: More than 3 billion in cost avoidance achieved by ESI first decade*. Retrieved from Department of Navy Chief Information Officer website:
<http://doncio.navy.mil/upload/0127WVH96937.pdf>

Smart CHESS Moves. (2010, March). Retrieved September 8, 2012, from Military Information Technology website: <http://www.military-training-technology.com/mit-home/231-mit-2010-volume-14-issue-2-march/2631-smart-chess-moves.html>

Snapshot: CHESS, Army's CHESS contract delivers big savings on hardware and software. (2011). Retrieved September 8, 2012, from Federal Computing Week website: <http://www.FCW.com/specialreportCHESS>

United States (2008), *Army Knowledge Management and Information Technology*, Army regulation 25-1, Washington, DC: Headquarters, Dept. of the Army.

Wardle, A. (2011, August). *Computer Hardware, Enterprise Software and Solutions Software 101*, Information Exchange Forum Session #5. Briefing presented at the 2011 LandWarNet conference, Tampa, FL.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Director
USACISA-P (JCISA)
PSC 303 Box 24
APO, AP 96204